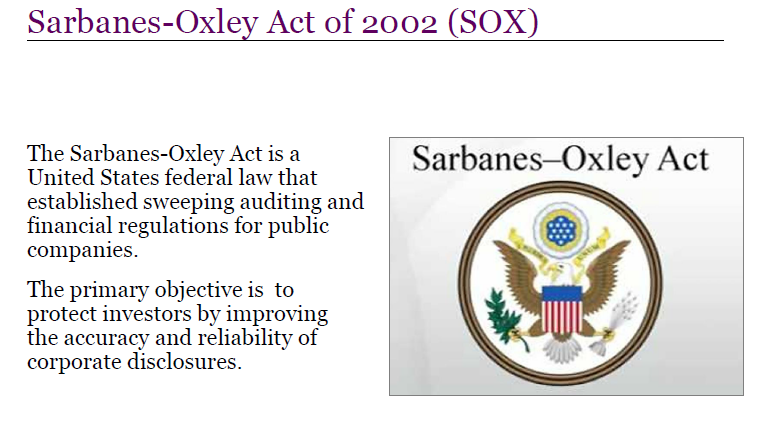
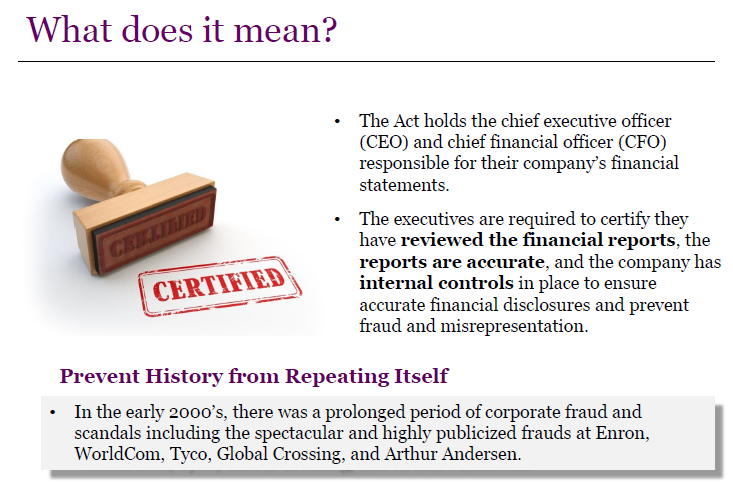
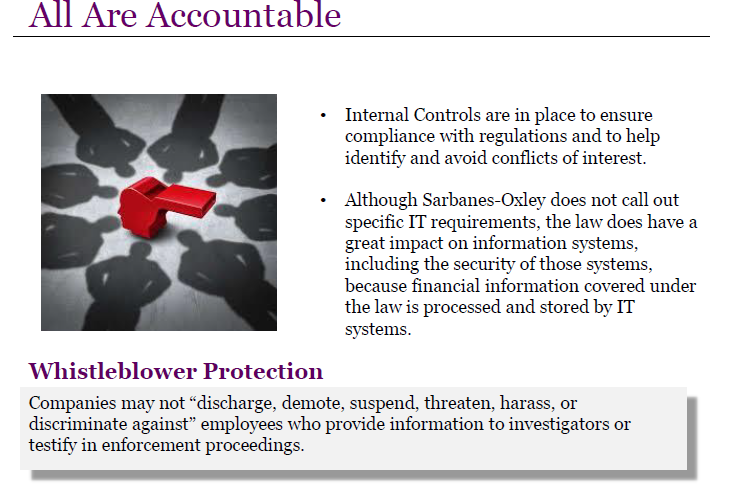
Sarbanes-Oxley (SOX)

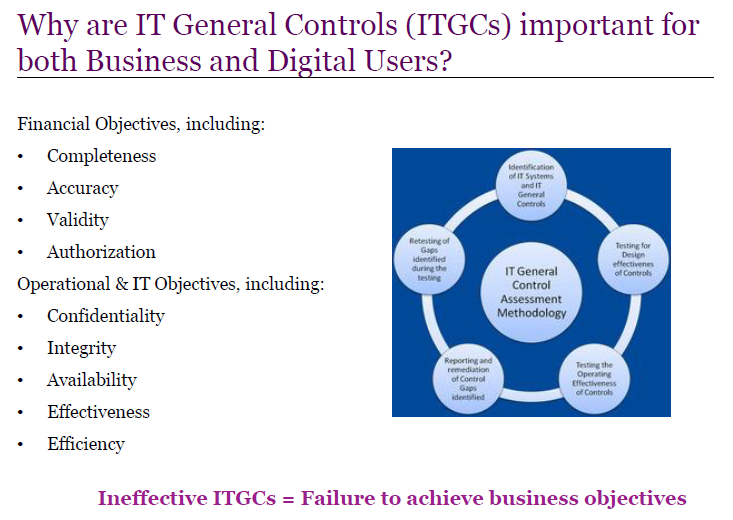
What is it and why is it important?



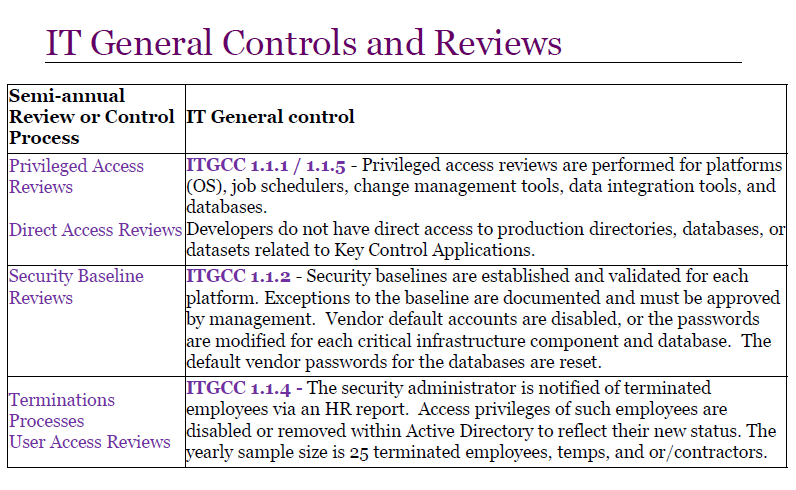


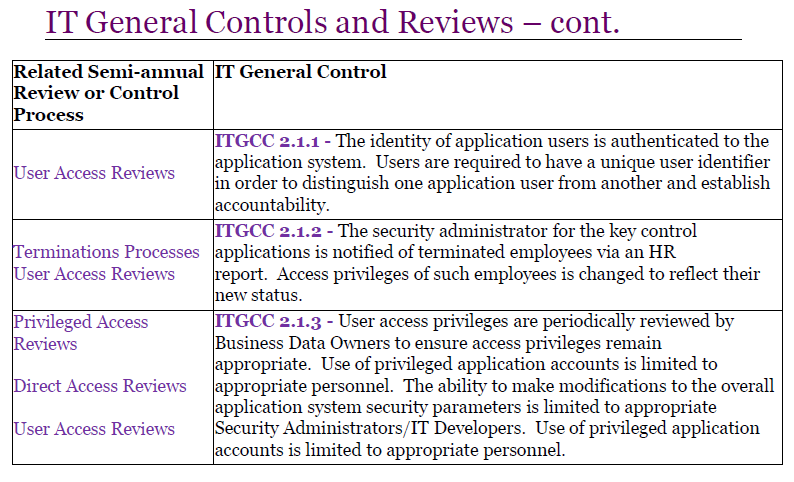


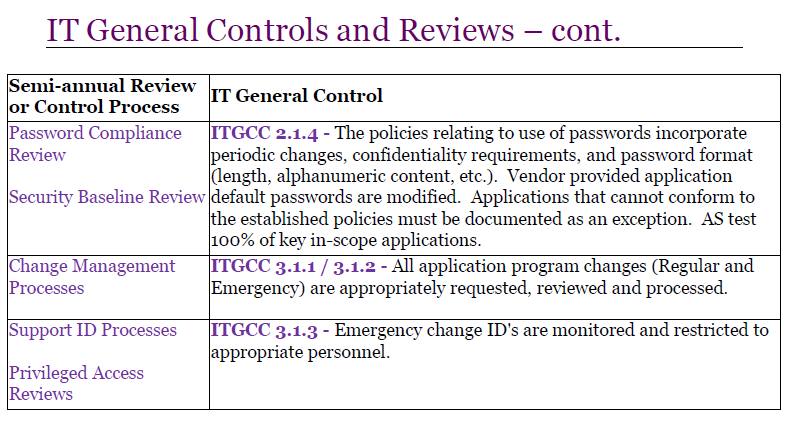


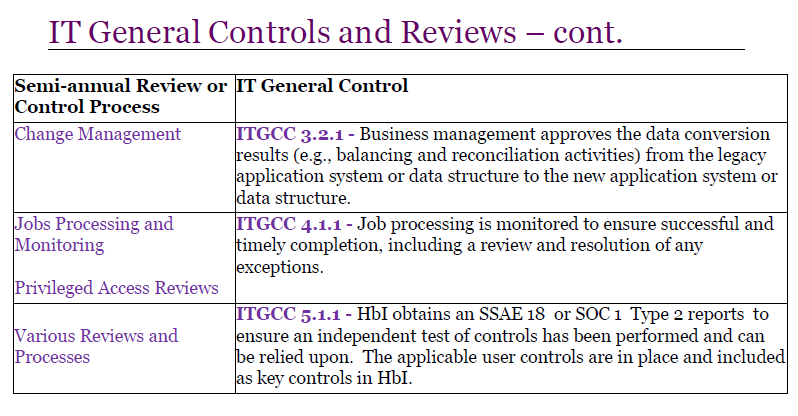


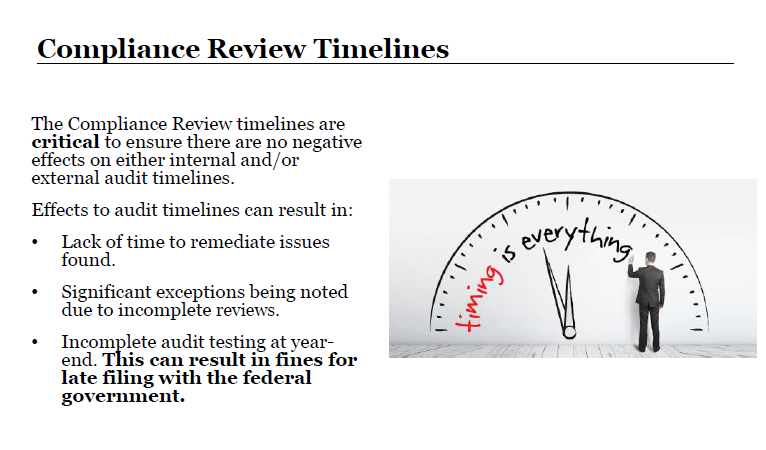


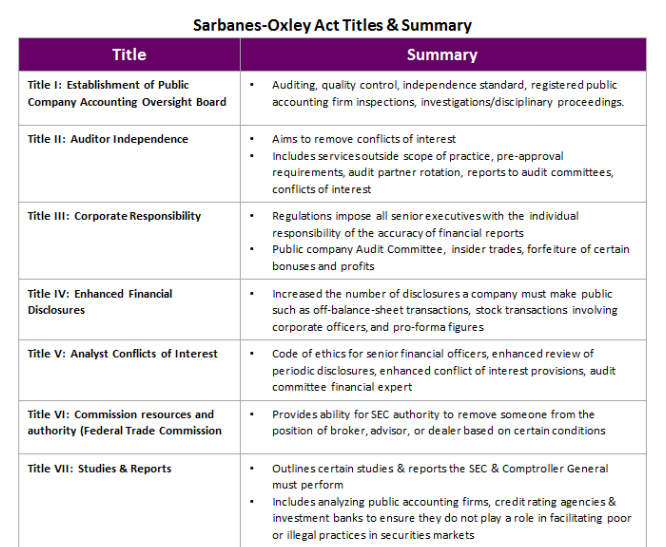


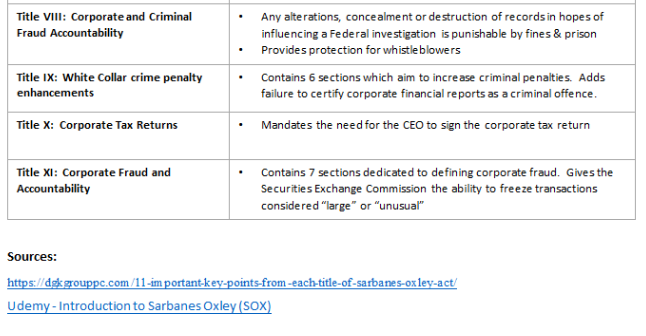












Acceptable Use of Information Systems & Equipment

# Summary

The key policy items contained in COMPANY NAME’s Acceptable Use of Information Systems & Equipment Policy (“Acceptable Use Policy”) are summarized below; policy details appear in the succeeding pages. COMPANY NAME systems and data are the property of COMPANY NAME and are to be used for business purposes. Limited personal use of COMPANY NAME computers and networks is permitted.

This global policy is applicable to all users of COMPANY NAME systems in compliance with applicable/local laws and regulations.

**Do not:**

* Use COMPANY NAME systems and equipment for anything illegal, or make unauthorized changes to COMPANY NAME or third party systems;
* Create, send, access, or retain any material that is offensive, illegal, or harassing;
* Use COMPANY NAME systems to conduct non-business activities such as promoting political or religious beliefs, gambling, etc.;
* Circumvent anti-virus software;
* Access any system using another user’s account;
* Connect any COMPANY NAME computing device to a non-COMPANY NAME network while also connected to the COMPANY NAME network;
* Open any files or click any links in an e-mail from an unknown, suspicious, or untrustworthy source – delete it and do not forward it;
* Connect to a non-COMPANY NAME system, including personal devices, unless approved by IT Management; and
* Allow non-employees to connect their laptops or other equipment to COMPANY NAME’s networks without prior approval.

**Do:**

* Scan removable media such as DVDs or USB drives with anti-virus software before use;
* Lock your workstations before leaving your desk to avoid unauthorized viewing or access;
* Use only licensed software and information products;
* Run approved anti-virus and firewall software on personally owned devices used to connect to COMPANY NAME webmail or other approved services;
* Physically secure all computing devices when not in use, particularly when traveling and/or out of the office; and
* Report all incidents, including loss or compromise of username and password, to the Customer Support Center (Ext. 9000).

# Introduction

## Background

COMPANY NAME provides information systems and equipment to employees and other individuals to enable them to discharge their assigned duties in a timely and effective manner. This policy defines the terms of acceptable use of COMPANY NAME’s information, systems and equipment.

## Purpose

Policies, standards, guidelines and baselines are defined to provide management direction and support for information security in accordance with business requirements and applicable/local laws and regulations.

## Objective

Objectives of this policy:

* To protect sensitive COMPANY NAME information from unauthorized disclosure and modification.
* To inform users of their responsibilities for compliance with COMPANY NAME’s information security policies.

## Applicability

This policy is applicable to all users of COMPANY NAME Systems and electronic equipment[[1]](#footnote-1).

# Acceptable Use Policy

COMPANY NAME systems and data are provided to employees to support business operations, including Internet/Intranet/Extranet-related systems, computer equipment, software, operating systems, storage media and network accounts (providing access to servers, electronic mail, internet browsing, FTP, and Instant Messaging systems). These systems and data are the property of COMPANY NAME and are to be used for business purposes.

## Unacceptable Use

COMPANY NAME systems and equipment **must not be used** for activities that do not comply with COMPANY NAME’s Information Security policies including, but not limited to:

* Illegal activities of any nature;
* Unauthorized changes to COMPANY NAME or third party systems;
* Creation, access or attempted access, transmission, storage, or retention of

material that could be considered sexually offensive or sexually or psychologically harassing in nature;

offensive language, jokes, or other written or pictorial material relating to an individual’s gender (including gender identity), race, religion, national origin, age, disability, sexual preference, or other characteristic protected by law;

material that disparages COMPANY NAME; its products; or its employees, officers, Board members, contractors, vendors, or suppliers; or

material that is contrary to the principles of COMPANY NAME’s Global Code of Conduct; or

any other material that could reasonably and negatively interfere with an individual’s work performance, make one uncomfortable, or create an offensive workplace environment.

* Pretending to be, misrepresenting, obscuring, suppressing, or replacing the identity of another person (referred to as “spoofing”);
* Interception of mail or any other business communication unless authorized by IT Security and Compliance (ITSC) and/or the Corporate Social Responsibility (CSR) group and consistent with applicable/local law and regulations;
* Access of confidential information without authorization by the owner of the information or in violation of system controls;
* Access of systems, transactions, mail, or other information using another user’s account/user ID;
* Changes of equipment configuration settings provided by COMPANY NAME; or
* Conducting activities related to:

Non-COMPANY NAME business except as allowed by the Reasonable Personal Use section of this policy;

Promoting political or religious beliefs;

Gambling;

Chain letters;

Junk mail and spam;

Hacking;

Harassment or bullying;

Discrimination as defined by COMPANY NAME’s Global Code of Conduct and related policies; or

Transmitting copyrighted or patented information without required permission.

Non-COMPANY NAME systems or equipment (personal equipment or equipment owned by another party) must not be connected to any COMPANY NAME network unless approved by ITSC and the IT Platform Management.

Users must not connect any COMPANY NAME computing device to any external network (e.g., publicly accessible wireless services or dial up) while also connected to the COMPANY NAME network. This is known as “split tunneling”. (Note that this does not prohibit accessing COMPANY NAME’s network though an approved remote access method such as VPN or SSL/VPN via an un-trusted network such as home, airport, and hotel networks.)

## Reasonable Personal Use

Limited personal use of COMPANY NAME computers and networks is allowed under the following conditions and applicable/local laws and regulations:

* User strictly adheres to all requirements of the Acceptable Use Policy described herein.
* Personal use does not interrupt or interfere with the job performance of the user or other employees.
* Personal use does not cause significant cost or drain of COMPANY NAME resources (e.g., excessive telephone or data usage, long-distance charges for calls, large group e-mails, streaming media[[2]](#footnote-2), and personal storage of data including MP3, MPEG or other multimedia files on COMPANY NAME equipment).

## Accountability

Users are responsible for all activities associated with their User ID. The following guidelines are provided to protect these IDs from unauthorized use:

* **Do**

use different passwords for COMPANY NAME and private purposes (e.g., password used to log in to COMPANY NAME Systems must be different from passwords used to log in to personal webmail accounts such as Yahoo, Gmail, etc.).

keep passwords confidential. (Users are responsible and accountable for activities with their accounts; and must never disclose passwords to anyone).

change passwords if compromise is suspected.

report compromise or suspected compromise of passwords.

use COMPANY NAME Systems only for COMPANY NAME business purposes (subject to Reasonable Personal Use section above).

* **Do not**

keep records of passwords in writing, in computer files, in PDAs or other storage unless they are securely stored and not likely to be found and used by others.

use macros, browser options for remembering passwords and similar programs to store or automatically submit passwords that are intended to be manually entered unless approved by IT Security and Compliance.

share COMPANY NAME-issued authentication credentials (user IDs, passwords, tokens, security certificates etc.) with other users even if they have similar levels of access in the system.

Users are responsible for the systems and data under their care. Users must report any loss of systems or data, or suspected loss of systems or data to the Security Incident Response Team (SIRT).

## Malicious Code

Users must adhere to and must consistently comply with security advisories and alerts provided by IT.

Removable media such as CDs, DVDs, USB drives and diskettes must be scanned for malicious code (viruses, ad-ware etc.) before use.

COMPANY NAME-owned and managed servers, desktops (PCs), laptops must run the latest COMPANY NAME approved version of anti-virus software configured to COMPANY NAME’s standard.

Users must not circumvent or attempt to circumvent anti-virus and other malicious code protection software.

COMPANY NAME permits a limited number of services (supporting SSL VPN connectivity) for use by any personal computer. Privately owned computers utilized for COMPANY NAME’s business in a home office for connecting remotely to COMPANY NAME webmail or other approved services must run approved anti-virus, firewall and anti-spyware software configured to COMPANY NAME’s standards. Privately owned mobile devices must be enabled through COMPANY NAME’s Mobile Device Management (MDM) solution to ensure effective management of mobile access to the COMPANY NAME network.

Employees must not allow non-employees (contractors, business partner personnel or others) to connect their laptops or other equipment to COMPANY NAME’s networks without prior approval by designated COMPANY NAME IT infrastructure or ITSC personnel.

COMPANY NAME staff and external parties must report all incidents and probable or potential incidents that may come to their attention. If the incident is related to malicious software, contact one of the following:

* For infections caused by a computer virus/malicious software or code, you must contact CSC[[3]](#footnote-3), or Security Incident Response Team (SIRT).
* For general queries relating to a computer virus/malicious software, code or e-mail attachments, contact the CSC.

COMPANY NAME staff and external parties must not write, generate, compile, copy, propagate, execute, or attempt to introduce any computer software/code designed to self-replicate, damage, or otherwise hinder the performance of any computer's hardware, memory, file system or software.

Where feasible, software or any executable file type must be run in an isolated test environment logically separated from COMPANY NAME’s production environment before being deployed in production.

## E-Mail Use

Users must never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source. Delete these messages immediately from the Inbox and Deleted Items folders.

Users must always delete spam, chain and other junk e-mail without forwarding.

Personal e-mail accounts (Yahoo, Gmail, Hotmail, etc.) may be accessed in accordance with the Reasonable Personal Use section of this policy and applicable/local laws and regulations. All protective measures described above also apply to the access of personal e-mail accounts since not doing so also exposes COMPANY NAME to the risk of malicious content.

Personal e-mail accounts may not be used in any way to conduct COMPANY NAME business or communicate COMPANY NAME information. This includes sending COMPANY NAME documents or forwarding COMPANY NAME emails to your personal email account or computers.

Do not send confidential information via e-mail unless the data is encrypted. When sending encrypted data via e-mail, do not send the encryption key using e-mail.

## Internet Use

Unless authorized by a documented and approved job requirement, users must not

* Download files from unknown or suspicious sources.
* Open documents with active content (such as macros).
* Visit or access any Internet site considered by COMPANY NAME to be inappropriate for the workplace.
* Circumvent or attempt to circumvent content filtering controls (i.e., software that defeats attempt to access sites such as those described in the third bullet above.)
* Upload, download, or otherwise transmit commercial software or any copyrighted material.
* Reveal or publicize COMPANY NAME confidential, proprietary, personal, or internal use only information that includes, but is not limited to: non-public financial information, personally identifiable information, new business and product ideas, marketing strategies and plans, pricing information, databases and information contained therein, employee information, organizational charts, internal announcements, customer lists, technical product information, computer software source codes, computer/network access codes, and business relationships (referred to collectively in this policy as “Confidential Information”).

Where digital certificates are used, the following activities must be performed while transferring information from Non-COMPANY NAME to COMPANY NAME Environments:

* The actual URL for the site being visited has been verified (i.e., by manually typing in the URL and not by just clicking a link sent in e-mail).
* Verify the validity and source of all digital certificates. Contact ITSC for further information regarding integrity checking.

## Network Use

User must not share folders with ‘read/write or full’ access. In case of absolute need, sharing must be enabled in a secure manner (using password, encryption tools, etc.) only on a need-to-access basis for the identified users and commensurate with the sensitivity of the information involved.

## Intellectual Property Rights (IPR)

Users must:

* Ensure legal (licensed) use of software and information products.
* Obtain explicit permission from the author or owner of IPR before reproducing or copying books, articles, reports, or other documents in full or in part.
* Acquire products only through COMPANY NAME authorized acquisition processes.

Users must not:

* Give any software or intellectual property to outsiders unless authorized.
* Make copies of licensed software under any circumstance without explicit permission from author or owner.
* Duplicate, convert to another format, extract from commercial recordings (film, audio etc.), decompile, or reverse engineer any intellectual property.
* Install any software on their workstation, servers, or other devices unless approved by authorized personnel from IT Security and Compliance.

## Removable Media Use

Users must:

* Ensure that removable media is maintained free from malicious and mobile code.
* Ensure that removable media under his/her custody is protected securely at all times to avoid theft and unauthorized access to data.
* Encrypt any confidential information stored on removable media with an encryption key that is maintained separately from the removable media.
* Report accidental loss and unauthorized access of removable media to the Security Incident Response Team (SIRT).
* Clarify the sensitivity of information, when in doubt, with the Information Asset Owners or ITSC.
* Not use personal/unapproved removable media to store COMPANY NAME data.
* Not use removable media to retain COMPANY NAME data in violation of COMPANY NAME’s Records Management Program policy.
* Not use COMPANY NAME-owned removable media for non-business purposes. (Refer to acceptable and personal use of COMPANY NAME assets above in this policy.)

## Clean Desk and Clear Screen Guidelines

Each User must follow a clean desk policy at his/her work area. Printed documents or removable media containing Confidential Information must not be kept in public view, or in an unlocked desk or cabinet while the user is not in the immediate vicinity of the material.

All documents containing Confidential Information must be shredded appropriately before disposal.

Users must ensure that they lock their workstations (e.g., desktop, laptop computer) before leaving their desks to avoid unauthorized viewing or access of Confidential Information or other workstation data.

All systems and electronic equipment must be physically secured when not in use.

## Information Handling

Users are responsible for the security of COMPANY NAME data. Users must ensure that documents, presentations, spreadsheets, or information in any other form are labeled, stored and transmitted based on the classification of the information as determined by the information asset owner.

Information not classified explicitly as “public” or “to be shared” must be assumed to be “Confidential Information” or for “Internal Use Only”. Users must not disclose such information to any external entity unless approved by information asset owners.

## Physical Security

Users of COMPANY NAME facilities must ensure that only the identification badges assigned to them are utilized for building or area access. Under no circumstances must they attempt to utilize access badges/privileges of others.

Users of COMPANY NAME facilities must not engage in “tailgating[[4]](#footnote-4)” and must ensure that others do not tailgate while they are accessing a company point-of-entry. Incidents relating to tailgating must be reported to the facility security team immediately.

Loss of an ID badge and/or access card must be immediately reported to the Facility Manager.

## User Backups

Backup of business-critical data that resides on the local hard drives of desktop/laptop computers must be created and managed by the end user. To ensure automated backup, COMPANY NAME encourages all users to store data on network drives (personal or shared).

## Monitoring, Violation Reporting, and Corrective Action

All e-mail created, sent, or received using COMPANY NAME facilities is the property of COMPANY NAME except those identified as private if permitted by local laws and under the conditions provided by applicable/local laws and regulations. If permitted by applicable/local laws and regulations and in compliance with them, COMPANY NAME may monitor e-mail messages created, sent internally and externally, received or stored on its systems.

COMPANY NAME will disclose communications, including text and images, to law enforcement agencies or administrations if legally required.

If permitted by applicable/local laws and regulations and in compliance with them, COMPANY NAME logs and monitors internet use. COMPANY NAME employees visiting a site deemed inappropriate may be subject to disciplinary action up to and including termination in accordance with applicable/local laws and regulations.

If permitted by applicable/local laws and regulations and in compliance with them, including requirements around frequency and notice, COMPANY NAME reserves the right to examine user storage systems (hard drives, network drives, removable media), web browser cache files, web browser bookmarks, and other information stored on, or passing through COMPANY NAME computers. For COMPANY NAME users in the U.S., such examination may occur at any time and without notice.

If permitted by applicable/local laws and regulations, information may be accessed by COMPANY NAME investigators, HR, and law enforcement agencies and may be used in conjunction with disciplinary or legal proceedings.

Users are encouraged to report all violations of this policy to their respective Code of Conduct Officer, the Global Ethics & Compliance Resource Line, or ITSC.

Violations of this policy may be subject to disciplinary action up to and including termination in accordance with applicable/local laws and regulations.

## Asset Labeling

COMPANY NAME Infrastructure maintains a cross reference list of all devices (including servers, routers, and switches). Specifically for those devices that participate in the credit card environment, visible labels are attached that define the business owner, technology owner, contact information and purpose of the device.

## Company Approved Products

The following end-user devices are authorized for use by COMPANY NAME employees:

* Personal Computers

Microsoft Windows-based PC – desktop and laptop

Lenovo PC/Laptop

Apple Macintosh

* Tablet Computers

Apple iPad

Microsoft Windows-based tablets

Android Operating System-based tablets

* Mobile Devices

Research In Motion Blackberry

Apple iPhone, iPod, Samsung and other Android devices

* Retail Store Users

IBM 4690 Store System

IBM 4690 Register

* Other computing platforms

Linux Operating System-based devices

* Other - Any device that supports access to COMPANY NAME corporate assets using standard network protocol(s) as permitted by ITSC

# Glossary

* **COMPANY NAME Systems:**

All business and support applications and enterprise services (e.g., e-mail, instant messaging, desk and mobile phone/voice mail, desktop and laptop computers, fax, scanning and photocopying devices, etc.) and

Supporting IT infrastructure such as databases, operating systems and network elements.

* **Users:** are people, employed or contracted by COMPANY NAME, having access to COMPANY NAME systems. Users also include business partners and corporate customer personnel authorized to access COMPANY NAME systems.
* **ITSC:** **I**nformation **T**echnology **S**ecurity and **C**ompliance
* **Information Asset Owners:** Business areas are owners of information assets just like other assets that belong to them. Therefore they are responsible for providing protection to them. The term ‘owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ’owner’ does not mean that the person actually has any property rights to the asset.

# Reference

* *System Access Control Policy*
* *Information Classification and Handling Policy*
* *Malicious Code Protection Policy*
* *Removable Media Security Policy*
* Backup Policy

1. Includes Tablets, Mobile Devices, Mobile Phones, Laptops, Telephones, etc. issued by COMPANY NAME and its subsidiaries [↑](#footnote-ref-1)
2. Streaming media is multimedia that is continuously received by, and normally displayed to, the end-user while it is being delivered by the provider. [↑](#footnote-ref-2)
3. Customer Support Center [↑](#footnote-ref-3)
4. "Tailgating" is where one or more people follow an authorized user of COMPANY NAME facility through a secured door or other entrance when the authorized person opens the door legitimately. This can be either with or without the authorized person's knowledge and/or consent. [↑](#footnote-ref-4)